UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/026,043 | 10/25/2001 | Huayan A. Wang | 1190 | 8635 |

7590 09/28/2005

Oleg F. Kaplun, Esq
FAY KAPLUN & MARCIN LLP
150 Broadway
Suite 702
New York, NY 10038

| EXAMINER | |
|---|---|
| KIM, JUNG W | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/026,043 | WANG ET AL. | |
| | Examiner | Art Unit | |
| | Jung W. Kim | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-21 are pending.

### *Claim Rejections - 35 USC § 112*

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. The term "likely" in claim 4 is a relative term which renders the claim indefinite. The term "likely" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The set of access points where the roaming device will roam is rendered indefinite. It is suggested to amend the claims as follows to overcome this 112 rejection: "... determining at least one access point of the access points using prediction algorithms to anticipate where the roaming device will roam ..." (Specification, pg. 5, paragraph 15).

### *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

### *Claim Rejections - 35 USC § 102*

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, 10 and 14-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Leung USPN 6,760,444 (hereinafter Leung '444); RFC 2138 is incorporated for inherent properties of RADIUS protocol.

9. As per claim 1, Leung '444 discloses a method for authenticating a roaming device with a network, comprising the steps of:

a. generating, by an authentication server of the network, authentication data associated with the roaming device (col. 7:36-38);

b. sending the authentication data to access points of the network, the access points being connected to the authentication server(7:38-44); and

c. when the roaming device roams to a particular access point of the access points, using the authentication data to locally authenticate the roaming device at the particular access point (7:54-61).

10. As per claim 2, the rejection of claim 1 under 35 U.S.C. 102(e) as being anticipated by Leung '444 is incorporated herein. (supra) In addition, the method further comprising the step of storing the authentication data in a memory arrangement of each of the access points (col. 7:58-59).

11. As per claim 3, the rejection of claim 1 under 35 U.S.C. 102(e) as being anticipated by Leung '444 is incorporated herein. (supra) In addition, the sending step includes the substeps of: encrypting the authentication data to selected access points of the access points (col. 7:3-5, the RADIUS protocol is used for transmitting the authentication data to and from the authentication server; RFC 2138, pg. 10, "Response Authenticator").

12. As per claim 4, the rejection of claim 3 under 35 U.S.C. 102(e) as being anticipated by Leung '444 is incorporated herein. (supra) In addition, the sending step includes the substep of determining at least one access point of the access points where the roaming device is likely to roam; and sending the encrypted authentication data to the at least one access points (col. 7:58; 4:40-56, a network comprising redundant Home Agents whether to provide homogenous access for a corporation or to provide backup transfers the security associations to the multiple Home Agents).

13. As per claim 5, the rejection of claim 3 under 35 U.S.C. 102(e) as being anticipated by Leung '444 is incorporated herein. (supra) In addition, the sending step includes the substep of sending the encrypted authentication data to all the access points (7:58; 4:40-56, a network comprising redundant Home Agents whether to provide homogenous access for a corporation or to provide backup transfers the security associations to the redundant Home Agents).

14. As per claim 10, Leung '444 discloses a method for authenticating a roaming device with a network, comprising the steps of:

d. connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network (7:10-21);

e. authenticating the roaming device with the authentication server (7:33-36);

f. generating authentication data for the roaming device(7:37-38);

g. distributing the authentication data to the first access point and a second access point of the network (7:43-44, 57-58; 4:40-56, a network comprising redundant Home Agents whether to provide homogenous access for a corporation or to provide backup transfers the security associations to the redundant Home Agents).; and

h. locally authenticating the roaming device upon a contact with the second access point using the distributed authentication data (7:54-61).

15. As per claim 14, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Leung '444 is incorporated herein. (supra) In addition, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points (col. 7:3-5, the RADIUS protocol is used for transmitting the authentication data to and from the authentication server; RFC 2138, pg. 10, "Response Authenticator").

16. As per claim 15, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Leung '444 is incorporated herein. (supra) In addition, the authentication server is a remote authentication dial –in user network (col. 7:3).

17. As per claim 16, Leung '444 discloses a system for authenticating a roaming device with a network, comprising:

i. an authentication server connected to the network (fig. 6, reference no. 602); and

j. first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and second access points including a memory arrangement capable of storing authentication data corresponding to the roaming device (4:40-56, a network comprising redundant Home Agents to provide homogenous access for a corporation and/or to provide backup),

k. wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point, and wherein the second access point locally authenticates the roaming device upon a contact of the roaming device with the second access point (7:43-44, 57-58; 4:40-56, a network comprising redundant Home Agents whether to provide homogenous access for a corporation or to provide backup transfers the security associations to the redundant Home Agents).

18. Claims 1-3, 6, 10-12, 14 and 16-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Singhai et al. USPN 6,851,050 (hereinafter Singhai '050).

19. As per claim 1, Singhai '050 discloses a method for authenticating a roaming device with a network, comprising the steps of:

l. generating, by an authentication server of the network, authentication data associated with the roaming device (col. 18:45-46);

m. sending the authentication data to access points of the network, the access points being connected to the authentication server(18:61-64); and

n. when the roaming device roams to a particular access point of the access points, using the authentication data to locally authenticate the roaming device at the particular access point (18:65-67).

20. As per claim 2, the rejection of claim 1 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the method further comprising the step of storing the authentication data in a memory arrangement of each of the access points (col. 18:64, 19:15-26).

21. As per claim 3, the rejection of claim 1 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the sending step includes the substeps of: encrypting the authentication data to selected access points of the access points (col. 18:64).

22. As per claim 6, the rejection of claim 1 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the method further comprising the preliminary steps of determining if the particular access point has authentication data associated with the roaming device; if the determination is positive,

proceed to the step of using the authentication data to locally authenticate the roaming device at the particular access point; and if the determination is negative, proceed to the step of generating, by an authentication server of the network, authentication data associated with the roaming device (fig. 15).

23. As per claim 10, Singhai discloses a method for authenticating a roaming device with a network, comprising the steps of:

o. connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network (18:40-45);

p. authenticating the roaming device with the authentication server (18:45);

q. generating authentication data for the roaming device(18:49-65);

r. distributing the authentication data to the first access point and a second access point of the network (18:60-65); and

s. locally authenticating the roaming device upon a contact with the second access point using the distributed authentication data (18:65-67).

24. As per claim 11, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the method further comprising the step of authenticating the roaming device with the authentication server if the local authentication of the roaming device fails (18:40-45; 19:20-23).

25. As per claim 12, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the distributing step further includes the substep of distributing an encrypted session key to the first and second access points (18:61-64).

26. As per claim 14, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points (18:64).

27. As per claim 16, Singhai '050 discloses a system for authenticating a roaming device with a network, comprising:

t. an authentication server connected to the network (fig. 14); and

u. first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and second access points including a memory arrangement capable of storing authentication data corresponding to the roaming device (18:66; 19:20-26),

v. wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point (18:61-67), and

w. wherein the second access point locally authenticates the roaming device upon a contact of the roaming device with the second access point (18:65-67).

28. As per claim 17, the rejection of claim 16 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the second access point authenticates the roaming device with the authentication server if the authentication data is not found in the memory arrangement of the second access point (fig. 15).

29. As per claim 18, the rejection of claim 16 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the second access points authenticates the roaming device with the authentication server if the local authentication of the roaming device at the second access point fails (19:20-26).

***Claim Rejections - 35 USC § 103***

30. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

32. Claims 7, 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Singhai '050 in view of Vij et al. USPN 6,452,910 (hereinafter Vij '910).

33. As per claim 7, the rejection of claim 6 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the step of using the authentication data to locally authenticate the roaming device further comprises reassociating the roaming device with the particular access point of the access points by providing identification information (fig. 15, reference nos. 1510 and 1520). However, Singhai '050 only discloses that the roaming device provides identification, and does not disclose that an exchange occurs between the roaming device and access points to reassociate. Vij '910 discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points utilizing a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver (col. 11:1-7). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming

device and the access point, since it is desirous to verify that the participants belong to the same local network (Vij, ibid). The aforementioned cover the limitations of claim 7.

34. As per claim 8, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the reasociating step further includes the substeps of:

x. searching a memory arrangement of the particular access point for the authentication data associated with the roaming device; and if the authentication data is found, performing a mutual authentication procedure between the roaming device and the particular access point (Singhai '050; Willins, paragraph 17).

35. As per claim 13, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, Singhai discloses the locally authenticating step further includes the substeps of:

y. providing identification data by the roaming device to the second access point; and correlating the identification data with the distributed authentication data (18:40-42 and 65-67).

36. However, Singhai '050 only discloses that the roaming device provides identification, and does not disclose exchanging identification between the roaming device and access points to reassociate. Vij discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points using a common link key to verify that the wireless device is authorized to access

the access point, and to ensure that the access point is the intended receiver (col. 11:1-7). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the participants of a transmission belong to the same local network (Vij, ibid). The aforementioned cover the limitations of claim 13.

37. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Singhai '050.

38. As per claim 9, the rejection of claim 1 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) In addition, the generating step further includes the steps of:

z. receiving an authentication request from the roaming device; determining that the roaming device can be granted access to network services; and generating an encrypted session key associated with the roaming device in the authentication server (18:40-64).

39. Singhai '050 does not expressly teach the authentication request is encrypted. However, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks. To prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an

authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication data to be transmitted securely to prevent the data from being stolen. The aforementioned cover the limitations of claim 9.

40. Claims 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Singhai '050 in view of Singhai et al. USPN 6,633,761 (hereinafter Singhai '761); RFC 2138 is incorporated to illustrate inherent properties of the RADIUS protocol.

41. As per claim 15, the rejection of claim 10 under 35 U.S.C. 102(e) as being anticipated by Singhai '050 is incorporated herein. (supra) Singhai '050 does not disclose the authentication server is a remote authentication dial-in user server. Singhai '761 discloses a seemless authentication procedure wherein a roaming user is authenticated by submitting a username and password to an access point (a HMP), and uses the RADIUS protocol to forward the username and password to an authentication server to authenticate the user (Singhai '761). Further, the RADIUS protocol is the de-facto standard for remote authentication as known in the art. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication server to be a RADIUS server, since it is desirous to implement protocols that have gained wide acceptance for reasons including, inter alia, standardization of design.

42. As per claim 19, Singhai '050 discloses a method for authenticating a roaming device with a network, comprising the steps of:

aa. with an authentication server, receiving an authentication request from a roaming device; with the authentication server, generating a session key associated with the roaming device; sending the session key to an access point of the network, the session key being encrypted with a second shared code; and utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point (18:40-67).

43. Singhai '050 does not expressly disclose the authentication request received from the roaming device is encrypted with a first shared code. Singhai '761 discloses a seemless authentication procedure wherein a roaming user is authenticated by submitting a username and password to an access point (a HMP), and uses the RADIUS protocol to forward the username and password to an authentication server to authenticate the user (Singhai '761, col. 8:64-9:7; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5). Further, it is well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication data to be transmitted securely to prevent the data from being stolen. The aforementioned cover the limitations of claim 19.

44. As per claim 20, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the method further comprising the step of sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point (18:64).

45. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Singhai '050 in view of Singhai '761, and further in view of Quick, Jr. USPN 6,178,506 (hereinafter Quick '506).

46. As per claim 21, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Singhai '050 discloses the method further comprising the steps of:

bb. generating a first key of the session key to perform authentication of the roaming device at the access point (fig. 15, reference no. 1500); and

cc. generating a second key of the session key to encrypt data exchanges between the roaming device and the access point (fig. 15, reference no. 1570a).

47. Singhai '050 does not expressly teach the first key as being different from the second key. Quick '506 discloses an authentication method wherein a first portion of a session key is used for authentication and a second portion of the session key is used for encryption. Since, the session key is larger then the required byte size necessary for authentication, the portion not used for authentication is used for encryption (col.

5:38-50). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first key generated from the session key to perform authentication and the second key generated from the session key to perform encryption to be different keys, since the protocols for authentication and encryption typically require different length keys (Quick '506, 5:45-50). The aforementioned cover the limitations of claim 21.

### *Conclusion*

48. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

49. WU et al. "Intelligent Handoff for Mobile Wireless Internet" discloses improved features of Wireless handoff transactions based on MWIN (home agents and foreign agents).

50. Rigney et al. RFC 2138.

51. Kim, Young "802.11b Wireless LAN Authentication, Encryption and Security".

52. Ala-Laurila et al. USPN 6,587,680.

53. Leung et al. USPN 6,760,444

54. Amada et al. US Patent Application Publication No. 2002/0120872.

### *Communications Inquiry*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

September 22, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100